

Secure Controlled Teleportation

Dan Kenigsberg^{1,*} and Tal Mor¹

¹Computer Science Department, Technion, Haifa 32000, Israel.

Several protocols for controlled teleportation were suggested by Yang, Chu, and Han [PRA **70**, 022329 (2004)]. In these protocols, Alice teleports qubits (in an unknown state) to Bob iff a controller allows it. We view this problem in the perspective of secure multi-party quantum computation. We show that the suggested entanglement-efficient protocols for m -qubit controlled teleportation are open to cheating; Alice and Bob may teleport $(m - 1)$ -qubits of quantum information, **out of the controllers' control**. We conjecture that the straightforward protocol for controlled teleportation, which requires each controller to hold m entangled qubits, is optimal. We prove this conjecture for a limited, but interesting, subset of protocols.

I. INTRODUCTION

Secure multi-party quantum computation (MPQC) protocol [3] allows n players to compute an agreed quantum circuit where each player has access only to his own arbitrary quantum input. A MPQC protocol has two phases: In the *sharing* phase, players dubbed dealers provide the other players with their initial state. In the *reconstruction* phase, the honest players help a designated player reconstruct the final state of the protocol. During the latter phase, only local operations and classical computation is available.

In this paper we view *controlled teleportation* as a special case of MPQC. A dealer named Carol hands Alice and Bob an (entangled) initial state $|\psi_{ABC}\rangle$. A second dealer, named David, provides Alice with an unknown m -qubit state ρ . The task of Alice and Bob is to reconstruct (teleport) ρ into Bob's hands, when Carol allows it. $|\psi_{ABC}\rangle$ is such that Carol controls whether the teleportation can take place. Carol and David are honest dealers. We call a controlled teleportation protocol *secure* if it is impossible for malicious Alice and Bob to teleport any part of ρ before the reconstruction phase. Namely, if Alice and Bob can build a state ρ' at Bob's hands which has non-trivial fidelity with ρ before the reconstruction phase, the protocol is insecure.

The straightforward solution to this problem, suggested in [7], is to use a procedure described in [4, 5]. First, Carol prepares the following $3m$ -qubit state and gives Alice and Bob their respective qubits

$$\begin{aligned} &\otimes_{i=1}^m |GHZ\rangle_{ABC(i)} = \\ &\otimes_{i=1}^m \left(|\phi^+\rangle_{AB(i)} |+\rangle_{C(i)} + |\phi^-\rangle_{AB(i)} |-\rangle_{C(i)} \right). \end{aligned} \quad (1)$$

(Here, and throughout the paper, we drop normalization factors for readability), $\{|\psi^\pm\rangle, |\phi^\pm\rangle\}$ are the four Bell-BMR[2] states, $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$, and $|GHZ\rangle_{ABC(i)} = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$ is the i th GHZ state shared among Alice, Bob

and Carol. Later, if Carol wishes to allow the teleportation, she measures her m qubits in the Hadamard basis, and publishes her results $c_i \in \{+, -\}$. Now, the state shared by Alice and Bob is $\otimes_{i=1}^m |\phi^{c_i}\rangle$ which can be freely used by them for teleportation.

On the other hand, if Carol abstains from participation, the state shared by Alice and Bob can be calculated by tracing over Carol's qubits

$$\begin{aligned} &\text{tr}_C \otimes_{i=1}^m |GHZ\rangle \langle GHZ|_{ABC(i)} = \\ &\otimes_{i=1}^m \left(|00\rangle \langle 00|_{AB(i)} + |11\rangle \langle 11|_{AB(i)} \right). \end{aligned} \quad (2)$$

We note here, that without the participation of Carol, the state shared by Alice and Bob becomes a classical correlation, which cannot facilitate quantum teleportation.

Ref. [7] provides a second protocol, in which Carol holds only one entangled qubit, aiming at the same task. This entanglement-efficient protocol can be stated as follows: Carol creates the following $2(m + 1)$ -qubit state and gives Alice and Bob their respective qubits

$$\otimes_{i=1}^m |\phi^+\rangle_{AB(i)} \otimes |\phi^+\rangle_{AC} + \otimes_{i=1}^m |\phi^-\rangle_{AB(i)} \otimes |\psi^+\rangle_{AC}. \quad (3)$$

Later, if Carol wishes to allow the teleportation, she measures her single qubit in the computational basis and publishes her result. Alice measures her own rightmost qubit in the computational basis. If it is equal to Carol's outcome, then Alice and Bob share $\otimes_{i=1}^m |\phi^+\rangle_{AB(i)}$. Otherwise, they share $\otimes_{i=1}^m |\phi^-\rangle_{AB(i)}$. Either way, they can safely teleport m qubits. On the other hand, if Carol abstains from participation, and if Alice and Bob continue the protocol exactly as planned, they can no longer teleport Alice's m -qubit message reliably, since they will create a mixed state [7, Eq. (11)] instead.

II. ALICE AND BOB CAN CHEAT CAROL

In fact, in the second protocol, even if Carol does not participate, malicious Alice and Bob can let Alice teleport any $(m - 1)$ -qubit state to Bob. The abstention of Carol mixes the shared state to create

$$\otimes_{i=1}^m |\phi^+\rangle \langle \phi^+|_{AB(i)} \otimes \mathbb{1}_A + \otimes_{i=1}^m |\phi^-\rangle \langle \phi^-|_{AB(i)} \otimes \mathbb{1}_A, \quad (4)$$

*Electronic address: danken@cs.technion.ac.il

where $\mathbb{1}$ is the totally mixed state in one qubit. Yet Alice and Bob can easily distill it [1]. Each of them has to relinquish his or her m th qubit and measure it in the computational basis. If their results coincide, they share $\otimes_{i=1}^{m-1} |\phi^+\rangle_{AB(i)}$; otherwise they share $\otimes_{i=1}^{m-1} |\phi^-\rangle_{AB(i)}$. Either way, they can safely teleport any $(m-1)$ -qubit state and thus reconstruct any m -qubit state with high fidelity.

It is important to note that [7] never claimed that Bob can learn *nothing* about Alice's state, and they stated openly that they did not "attempt a comprehensive study of the security against all possible forms of eavesdropping and/or cheating". However, it is equally important to note that their efficient protocol for multiqubit quantum information teleportation via the control of an agent, is insecure. The same malady affects their protocol for multiple controllers (see Section IV).

III. CAROL NEEDS m ENTANGLED QUBITS

When Carol held a single qubit entangled to Alice and Bob, she could control only one of their qubits, and not the rest. We believe that this is not an accident. We *conjecture* that Carol must have at least m entangled qubits with Alice and Bob if she wants to completely control their ability to teleport an m -qubit state.

We prove a special case of this conjecture. We define a limited form of secure controlled teleportation. In the limited form, we assume three additional limitations. (a) The initial state shared by Alice, Bob and Carol is pure.[8] (b) If Carol abstains, the remaining state $\rho_{AB} = \text{tr}_C |\psi_{ABC}\rangle \langle \psi_{ABC}|$ is separable.[9] (c) In the reconstruction phase, Carol performs her measurement on the shared state without obtaining any prior information from Alice and Bob; Alice and Bob do not help Carol to assist them.[10]

These limitations are not true in general, since the initially-shared state may be mixed, since a bound-entangled state is probably equally unhelpful for Alice and Bob if they want to perform teleportation, and since the reconstruction phase can be more complex. Note that these limitations leave enough room for interesting protocols. Specifically, the protocols of [7] satisfy limitations (a) and (c), and the ones not satisfying (b) can be cheated because of that.

Limitation (c) means that the highest value of entanglement that Alice and Bob can create between them with the help of Carol is $EoA^1(\rho_{AB})$, the entanglement of assistance, which in turn is limited by $EoA^\infty(\rho_{AB})$. Recently, Smolin, Verstraete, and Winter [6] showed that

$$EoA^\infty(\rho_{AB}) \leq \min(S(A), S(B)). \quad (5)$$

Let us now assume that a secure limited controlled teleportation protocol exists, i.e. there exists $|\psi_{ABC}\rangle$ so that $\rho_{AB} = \text{tr}_C |\psi_{ABC}\rangle \langle \psi_{ABC}|$ is separable, while $EoA^1(\rho_{AB}) \geq m$. Since ρ_{AB} is separable, $S(\rho_{AB}) \geq$

$\max(S(A), S(B))$. We conclude that

$$\begin{aligned} S(\rho_{AB}) &\stackrel{(b)}{\geq} \max(S(A), S(B)) \\ &\geq \min(S(A), S(B)) \stackrel{[6]}{\geq} EoA^\infty(\rho_{AB}) \\ &\stackrel{(c)}{\geq} EoA^1(\rho_{AB}) \geq m. \end{aligned} \quad (6)$$

But since $|\psi_{ABC}\rangle$ is pure, $S(\rho_{AB})$ is exactly the initial entanglement of Carol with Alice and Bob. Thus, a limited controlled teleportation protocol requires Carol to hold no less than m entangled bits—just as in the straightforward protocol.

IV. MULTIPLE CONTROLLERS

In an extended problem presented in [7], Carol is replaced by n controllers: If all the controllers participate, Alice can teleport an m -qubit message to Bob. But even if a single controller abstains, the teleportation has to be impossible.

In the straightforward protocol achieving this, the controllers prepare the following $(n+2)m$ -qubit state and give each participant his or her respective qubits

$$\begin{aligned} \otimes_{i=1}^m |GHZ\rangle_{ABC^n(i)} = \\ \otimes_{i=1}^m \left(|\phi^+\rangle_{AB(i)} H^{\otimes n} \sum_{\text{even } |x|} |x\rangle_{C^n(i)} + \right. \\ \left. |\phi^-\rangle_{AB(i)} H^{\otimes n} \sum_{\text{odd } |x|} |x\rangle_{C^n(i)} \right) \end{aligned} \quad (7)$$

where $H^{\otimes n}$ is the Hadamard transform on n qubits, and the summations are over the n -bit strings x whose Hamming weight $|x|$ is even (odd). Later, when all the controllers wish to allow the teleportation, each of them apply the Hadamard transform to her first qubit, measures it in the computational basis, and publishes her result. If the number of "1"s published by all controllers is even (odd), Alice and Bob share $|\phi^+\rangle$ ($|\phi^-\rangle$). Either way, they can safely teleport one qubit. This is repeated on the $m-1$ sets of remaining qubits.

On the other hand, if even a single controller abstains, the complete state becomes a classical correlation, unworthy for teleportation.

In this protocol each controller initially holds m entangled bits with the rest of the system. Much like as in the case of a single controller, the protocol cannot be improved by another protocol of the limited form.

If all n controllers participate, they can be thought of as one, and $m \leq EoA(\rho_{AB}) \leq \min(S(A), S(B))$.

If one of the controllers (C') abstains, we require that $\rho_{ABC^{n-1}}$ would become separable. Again, this means that each controller's entanglement with the rest of the system $S(C') = S(\rho_{ABC^{n-1}})$ has to be

more than $\max(S(A), S(B))$ and certainly more than $\min(S(A), S(B)) \geq m$.

Any limited controlled teleportation protocol that tries to be more entanglement-efficient than that, is insecure. For example, in the shared state suggested in [7, Eq. (21)]

$$\begin{aligned} & \otimes_{i=1}^m |\phi^+\rangle_{AB(i)} \otimes |GHZ_+\rangle_{AC^n} + \\ & \otimes_{i=1}^m |\phi^-\rangle_{AB(i)} \otimes |GHZ_-\rangle_{AC^n} \end{aligned} \quad (8)$$

(where $|GHZ_{\pm}\rangle = |0\dots 0\rangle \pm |1\dots 1\rangle$ is an $n+1$ qubit state share by Alice and the n controllers) there is only one bit of entanglement between the group of all controllers

and the Alice and Bob pair. Therefore, Alice and Bob can again ignore the controllers and remain with a state useful for teleportation.

V. ACKNOWLEDGMENTS

We thank Amir Kalev and Gili Bisker for discussing this paper with us and for their valuable comments, and for the support of the Israeli MOD Research and Technology Unit.

-
- [1] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76(5):722–725, 1996.
 - [2] S. L. Braunstein, A. Mann, and M. Revzen. Maximal violation of Bell inequalities for mixed states. *Phys. Rev. Lett.*, 68:3259–3261, 1992.
 - [3] C. Crépeau, D. Gottesman, and A. Smith. Secure multi-party quantum computation. In *34th ACM Symposium on the Theory of Computing (STOC)*, pages 643–652, 2002.
 - [4] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829, 1999.
 - [5] A. Karlsson and M. Bourennane. Quantum teleportation using three-particle entanglement. *Phys. Rev. A*, 58:4394, 1998.
 - [6] J. A. Smolin, F. Verstraete, and A. Winter. Entanglement of assistance and multipartite state distillation. *Phys. Rev. A*, 72:052317, 2005.
 - [7] C.-P. Yang, S.-I. Chu, and S. Han. Efficient many-party controlled teleportation of multiqubit quantum information via entanglement. *Phys. Rev. A*, 70:022329, 2004.
 - [8] In general, this state could have been mixed.
 - [9] In general, it is probably enough to assume that the state without Carol is not distillable, namely either separable or bound-entangled.
 - [10] In general, Carol’s measurements can depend on the outcome of Alice and Bob’s measurements; The reconstruction phase can be more complex.